

REMARKS

Claims 1-6, 11, 17, 18, 20, 21, 25, 27, 28, 31 and 33-46 were pending prior to this paper. In this paper, the Applicant has further amended the application by:

- cancelling claim 45 and remedying a double inclusion of claim 36 by cancelling the second claim 36;
- amending claims 1, 4, 34, 35, 42-44 and 46; and
- adding new claims 47-54.

The amendments to claims 1, 4, 34, 35, 42-44 and 46 and the subject matter of new claims 47-54 are submitted to contain no new matter and to be completely supported by the application as filed.

As a result of these amendments, claims 1-6, 11, 17, 18, 20, 21, 25, 27, 28, 31, 33-44 and 46-54 are currently pending.

Claim 45

The Office Action raises 35 U.S.C. § 112 in connection with claim 45. The Applicant has cancelled claim 45, thereby obviating the Examiner's rejection.

Double inclusion of claim 36

In the amendment dated 30 March 2006, the Applicant mistakenly included two claims numbered 36. The Applicant has cancelled the second such claim 36. Only one claim 36 remains in the listing of claims presented above.

Claims 1, 3, 17, 21, 25 and 34-42

The Office Action raises the combination of US patent No. 6,052,780 (Glover) and US patent No. 6,055,314 (Spies et al.) in connection with claims 1, 3, 17, 21, 25 and 34-42. The Applicant submits that claims 1, 3, 17, 21, 25 and 34-42 patentably distinguish the combination of Glover and Spies et al.

On page 4 of the Office Action, the Examiner correctly states that Glover does not disclose the previous claim 1 feature of "receiving the decryption key from the remote

server, the decryption key itself encrypted with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key.” The Applicant has made minor amendments to this claim 1 feature for clarity. Claim 1 (as amended) recites “receiving the decryption key from the remote server at the user computing device, the decryption key itself encrypted at the remote server with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key.” The Applicant submits that Spies et al. fail to remedy this deficiency.

On page 5 of the Office Action, the Examiner expresses the view that Spies et al. disclose this claim 1 feature at col. 6, ln. 55-58; col. 8, ln. 35-57; col. 11, ln. 40-45 and col. 14, ln. 59-63. This view is incorrect. Figure 2 shows the Spies et al. system, wherein an IC card (50) sends its credential (54) to a merchant computing unit (44) and the merchant computing unit (44) returns a cryptographic program key (56) to the IC card (50). The encryption protocol taught by Spies et al. is described in col. 7 and col. 8. At col. 8, ln. 26-57, Spies et al. describe how “decryption capabilities” (which include the policy and program key (56) for ordered video content) are encrypted and sent from the merchant computing unit (44) to IC card (50). The Spies et al. “decryption capabilities” are described as being “encrypted using the public exchange key of the IC card” (see col. 8, ln. 39-40) and subsequently “transferred to the IC card directly” (col. 8, ln. 44). Spies et al. then disclose that “[t]he IC card decrypts the policy and program key using its own private exchange key” (col. 8, ln. 45-46). This portion of Spies et al. clearly discloses that the Spies et al. system uses one key (the “public exchange key of the IC card”) to encrypt the “decryption capabilities” and a second key (the “private exchange key” of the IC card) to decrypt the “decryption capabilities”.

In direct contrast, claim 1 (as amended) recites “receiving the decryption key from the remote server at the user computing device, the decryption key itself encrypted at the remote server with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key.” Thus, in accordance with claim 1, a single key (the “user key”) is used to encrypt the decryption

key at the remote server and to decrypt the decryption key at the user computing device. Spies et al. does not teach or suggest this claim 1 feature.

Based on this reasoning, claim 1 is submitted to patentably distinguish the combination of Glover and Spies et al. Claims 3, 17, 21, 25 and 34-42 depend from claim 1 and are submitted to patentably distinguish the combination of Glover and Spies et al. for at least this reason.

Claims 2, 18 and 20

The Office Action raises the combination of Glover, Spies et al. and US patent No. 6,564,248 (Budge et al.) in connection with claims 2, 18 and 20. The

Claims 2, 18 and 20 depend from claim 1. As discussed above, neither Glover nor Spies et al. disclose the claim 1 feature of “receiving the decryption key from the remote server at the user computing device, the decryption key itself encrypted at the remote server with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key.” Budge et al. fails to remedy this deficiency.

Accordingly, the Applicant submits that claims 2, 18 and 20 patentably distinguish the combination of Glover, Spies et al. and Budge et al.

Claims 27 and 40

The Office Action raises the combination of Glover, Spies et al. and US patent No. 6,385,596 (Wiser et al.) in connection with claims 27 and 40.

Claims 27 and 40 depend from claim 1. As discussed above, neither Glover nor Spies et al. disclose the claim 1 feature of “receiving the decryption key from the remote server at the user computing device, the decryption key itself encrypted at the remote server with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key.” Wiser et al. fails to remedy this deficiency.

Accordingly, the Applicant submits that claims 27 and 40 patentably distinguish the combination of Glover, Spies et al. and Wiser et al.

Additional comments regarding claims 17, 18 and 34-41

Claims 17, 18 and 34-41 depend from claim 1 and are submitted to be patentable over the combination of Glover and Spies et al. for the reasons set out above.

In addition, however, claim 34 (as amended) recites “generating the user key at the user computing device.” The Examiner expresses the view that Spies et al. disclose this claim 34 feature at col. 11, ln. 40-45 and/or at col. 8, ln. 25-41. With respect, the Applicant submits that this view is incorrect.

At col. 11, ln. 40-45, Spies et al. describe how IC card (50) “stores” two asymmetric pairs of public and private cryptography keys (114). Storage of a cryptographic key (as disclosed by Spies et al.) is not equivalent to “generating” the user key at the user computer device as recited in claim 34.

As discussed above, col. 8, ln. 25-41 of Spies et al. describe how an “decryption capabilities” (which include the policy and program key for ordered video content) are encrypted and sent from the merchant computing unit (44) to IC card (50). Nowhere in this passage do Spies et al. teach or suggest “generating” the user key at the user computer device as recited in claim 34.

The Applicant submits that claim 34 patentably distinguishes the combination of Glover and Spies et al. for this additional reason. Claims 17, 18 and 35-41 depend from claim 34 and are submitted to also patentably distinguish the combination of Glover and Spies et al. for this additional reason.

Additional comments regarding claims 17, 18 and 35-42

Claims 17, 18 and 35-42 depend from claim 1 and are submitted to be patentable over the combination of Glover and Spies et al. for the reasons set out above.

In addition, however, claims 35 and 42 (as amended) both recite “wherein decrypting the media content at the user computing device using the integral decryption engine and the decryption key comprises using the user key to decrypt the decryption key”

and to thereby obtain a decrypted decryption key.” The Examiner expresses the view that Spies et al. disclose this claim 35 feature at col. 16, ln. 20-30. With respect, the Applicant submits that this view is incorrect.

As discussed above, Spies et al. clearly disclose a system which uses one key (the “public exchange key of the IC card”) to encrypt the “decryption capabilities” and a second key (the “private exchange key” of the IC card) to decrypt the “decryption capabilities”. Col. 16, ln. 20-30 of Spies et al. merely confirms that the Spies et al. process involves encrypting a program key with the “public exchange key” of the IC card (50) and, at the IC card (50), decrypting the program key using a “private exchange key”.

In direct contrast, claims 42 and 35, incorporate the claim 1 feature of “receiving the decryption key from the remote server at the user computing device, the decryption key itself encrypted at the remote server with a user key” and claims 35 and 42 both recite “using the user key to decrypt the decryption key and to thereby obtain a decrypted decryption key.” Spies et al. (which teaches the use of a public key for encryption and a private key for decryption) does not teach or suggest this combination of features from claims 35 and 42.

The Applicant submits that claims 35 and 42 patentably distinguish the combination of Glover and Spies et al. for this additional reason. Claims 17, 18 and 36-41 depend from claim 35 and are submitted to also patentably distinguish the combination of Glover and Spies et al. for this additional reason.

Claims 4-6, 11, 28, 31, 43 and 44

The Office Action raises the combination of Glover, Spies et al. and Budge et al. in connection with claims 4-6, 11, 28, 31, 43 and 44. The Applicant submits that claims 4-6, 11, 28, 31, 43 and 44 patentably distinguish the combination of Glover, Spies et al. and Budge et al.

Claim 4 (as amended) recites “receiving a single file ..., the single file executable independently of other programs to: obtain a decryption key from a remote server, the decryption key itself encrypted at the remote server with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to

decrypt the decryption key.” As discussed above in relation to claim 1, the combination of Glover and Spies et al. do not disclose this combination of features. More particularly, neither Glover nor Spies et al. disclose the use of a single "user key" to encrypt a decryption key at a remote server and then to decrypt the decryption key at a user computing device as recited in claim 4. Budge et al. fail to remedy this deficiency.

Based on this reasoning, the Applicant submits that claim 4 patentably distinguishes the combination of Glover, Spies et al. and Budge et al. Claims 5, 6, 11, 28, 31, 43 and 44 depend from claim 4 and are submitted to be patentable over the cited prior art for at least this reason.

Claim 33

The Office Action raises the combination of Glover, Spies et al., Budge et al. and Wiser et al. in relation to claim 33.

Claim 33 depends from claim 4. As discussed above, neither Glover, nor Spies et al., nor Budge et al. disclose the claim 4 feature of “receiving a single file ..., the single file executable independently of other programs to: obtain a decryption key from a remote server, the decryption key itself encrypted at the remote server with a user key, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device such that the user computing device can use the user key to decrypt the decryption key.” Wiser et al. fails to remedy this deficiency.

Accordingly, the Applicant submits that claim 33 patentably distinguishes the combination of Glover, Spies et al., Budge et al. and Wiser et al.

Additional Comments regarding claims 43 and 44

Claims 43 and 44 depend from claim 4 and are submitted to be patentable over the combination of Glover, Spies et al. and Budge et al. for the reasons set out above.

In addition, however, claim 43 (as amended) recites “wherein execution of the single file causes the user computer device to generate the user key at the user computing device.” The Examiner expresses the view that Spies et al. disclose this claim 43 feature at col. 15, ln. 60-67. The Applicant respectfully submits that this view misinterprets the teachings of Spies et al.

At col. 15, ln. 60-67, Spies et al. describe how a headend server (210) handles a purchase order (240) and payment instructions (242) using a private exchange key and verifies a digital signature using the public signing key of the IC card (50) contained in the credentials (54). This passage from Spies et al. does not teach or suggest that either headend server (210) or IC card (50) executes a file in order to “generate the user key at the user computing device” as recited in claim 33. Moreover, Spies et al. specifically teach (in Figure 6 and at col. 11, ln. 40-46) that IC card (50) “stores” two asymmetric pairs of public and private cryptography keys (114). Storage of a cryptographic key (as disclosed by Spies et al.) is not equivalent to executing a file which “generate[s]” the user key at the user computer device as recited in claim 43.

The Applicant submits that claim 43 patentably distinguishes the combination of Glover, Spies et al. and Budge et al. for this additional reason. Claim 44 depends from claim 43 and is submitted to also patentably distinguish the combination of Glover, Spies et al. and Budge et al. for this additional reason.

Additional comments regarding claim 44

Claim 44 depends from claim 4 and is submitted to be patentable over the combination of Glover, Spies et al. and Budge et al. for the reasons set out above.

In addition, however, claim 44 (as amended) recites “using the user key to decrypt the decryption key and to thereby obtain a decrypted decryption key.” The Examiner expresses the view that Spies et al. disclose this claim 44 feature at col. 16, ln. 20-30. This view is incorrect.

As discussed above, Spies et al. clearly disclose a system which uses one key (the “public exchange key of the IC card”) to encrypt the “decryption capabilities” and a second key (the “private exchange key” of the IC card) to decrypt the “decryption capabilities”. Col. 16, ln. 20-30 of Spies et al. merely confirms that the Spies et al. process involves encrypting a program key with the “public exchange key” of the IC card (50) and, at the IC card (50), decrypting the program key using a “private exchange key”.

In direct contrast, claim 44 incorporates the claim 4 feature of “receiving a single file ... the single file executable independently of other programs to: obtain a decryption key from a remote server, the decryption key itself encrypted at the remote server with a user key” and claim 44 recites “using the user key to decrypt the decryption key and to thereby obtain a decrypted decryption key.” Spies et al., which teaches the use of a public key for encryption and a private key for decryption, does not teach or suggest this claim 44 combination of features.

The Applicant submits that claim 44 patentably distinguishes the combination of Glover, Spies et al. and Budge et al. for this additional reason.

Claim 46

The Office Action raises the combination of Glover and Spies et al. in connection with claim 46. The Applicant submits that claim 46 patentably distinguishes Glover and Spies et al.

Claim 46 (as amended) recites the combination of “generating a user key at the user computing device, the user key bonded to the user computing device by being based at least in part on one or more characteristics of the user computing device” and “receiving the decryption key from the remote server at the user computing device, the decryption key itself encrypted at the remote server with the user key such that the user computing device can use the user key to decrypt the decryption key.” The Examiner correctly suggests on page 4 of the Office Action that Glover does not disclose this combination of features. As discussed above in relation to claim 1, Spies et al. fail to remedy this deficiency.

The Applicant submits that the claim 46 feature of “generating a user key at the user computing device,” which is not discussed in the Office Action, is not shown by the combination of Glover and Spies et al. As discussed above, Spies et al. specifically teach (in Figure 6 and at col. 11, ln. 40-46) that IC card (50) “stores” two asymmetric pairs of public and private cryptography keys (114). Storage of a cryptographic key (as disclosed by Spies et al.) is not equivalent to “generating a user key at the user computing device” as recited in claim 46.

On the basis of this reasoning, the Applicant submits that claim 46 patentably distinguishes the combination of Glover and Spies et al.

New claims 47-54

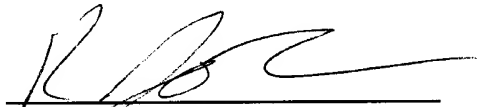
The Applicant has added new claims 47-54. The Applicant submits that new claims 47-54 are completely supported by the Application as originally filed and add no new matter. The Applicant submits that new claims 47-54 patentably distinguish the prior art of record.

Conclusions

The Applicant submits that this application is now in condition for allowance and respectfully requests reconsideration and allowance of this application in light of the foregoing amendments and comments.

Respectfully submitted,
OYEN WIGGS GREEN & MUTALA LLP

By:



Richard A. Johnson

Registration No. 56,080

tel: 604.669.3432 ext. 9046

fax: 604.681.4081

e-mail: tardocket@patentable.com